BUREAU OF CONSUMER PROTECTION Consumer Facts

Protecting Wisconsin Consumers for 75 Years

GPS safety tips

A growing number of smartphones and other mobile devices have Global Positioning System (GPS)-based locator functions built in. The technology allows mobile device users to locate a business, check local traffic or weather, keep track of their children, and more. Mobile devices also use this technology to automatically add geolocation information to pictures taken with the onboard cameras – a practice known as "geotagging."

Most people do not realize that the geotagging of photos is set as a default action on their new mobile devices. As a result, many individuals do not turn off the function and unknowingly share a great deal of information about their exact location by simply snapping photos and posting them online with their mobile devices. Criminals are paying attention to those mistakes.

In addition to spying, stalking or theft, it is critical to understand that location and sharing technology on mobile devices can lead to **identity theft** if location information is made publicly available. For example, if smartphone messages that share your location are linked to your Facebook and Twitter accounts and you share your network with a lot of people, you could be sharing location information with people you may not trust and who may misuse the information for their own purposes.

Here is how it works

A GPS receiver built into your mobile device feeds location data into applications that let you find out where your friends are – and it lets them find you. Location services also allow you to map directions for driving, locate a nearby restaurant or access local weather reports while on the go. Some of those services rely on unique location data to provide accurate results; this data may be collected through your phone's GPS or through a nearby Wi-Fi access point or cellular tower.

The device can also use GPS technology to automatically embed information about the precise spot where a photo was taken with the onboard camera ("geotagging"). So when you text, email or post a picture to a photo-sharing site or social network page, that geographical data sticks with the photo when it goes out to others.

Facebook and Twitter can also take advantage of the GPS technology on your mobile device by geotagging status messages and tweets posted from that device.

These seemingly harmless functions actually provide criminals with the ability to reverse-search (or "reverse-geocode") the data of the posted photos, Twitter feeds, Facebook activities, and location searches that involve GPS-related location-sharing services from your mobile device.

By reverse-geocoding and conducting alternative searches on you without your consent or acknowledgement, the criminals are piecing together information that they can use to steal your identity (and more).

How to use location services safely

Choose the level of privacy that best fits your situation.

Fine-tune location settings

- Before you turn on geotagging for any of your social networking accounts, think carefully on whether or not you want to share this information with everyone on those networks.
- Check your phone settings for any application you have downloaded that uses your location to provide a service. Most people have agreed to share this information without even realizing it.
- Only geotag photos when you need to mark them with your location. Note: it is safer not to geotag photos of your children or your home.
- Consider disabling location services on your phone completely, or at minimum, limit the number of applications you allow to access this information. By doing this you will limit features like maps, bus-route data, or services that allow you to watch over your children.

Restrict who knows your location

- Only share your location with people you know and trust.
- Disable options that allow other users to share your location, or “check you in” on your behalf.

Pay attention to where and when you check in. Think before checking in by asking yourself a few questions

- Does it enhance or harm your reputation?
- Will it put others at risk? For example, are you “checking in” from your home, your kids’ school, or a friend’s house?
- Are you alone? If so, is it safe?

The easiest way to stop your mobile device from posting your information for everyone to see is to disable the geotagging setting. Usually you need to open the camera application, go into the settings and set the location setting to off. Since each mobile device may do this differently, it is best to consult the manufacturer of your phone or device for detailed instructions. For more information on protecting your children online, visit the Bureau of Consumer Protection’s website at datcp.wi.gov.

For regular updates and information on consumer protection and identity theft issues, visit the Wisconsin Bureau of Consumer Protection’s Facebook page and be sure to “like” us and follow us on Twitter.

For more information or to file a complaint, visit our website or contact the Bureau of Consumer Protection.

Bureau of Consumer Protection
2811 Agriculture Drive
PO Box 8911
Madison WI 53708-8911

E-MAIL: DATCPWisconsinPrivacy@wi.gov

WEBSITE: datcp.wi.gov

(800) 422-7128

FAX: (608) 224-4677

TTY: (608) 224-5058